IA 3

Emergency Operations Plan – Incident Annex 3

Cyber Incident

Section 1: Introduction

1.1 Lead Agencies

- Maine Department of Defense, Veterans, and Emergency Management (DVEM) - Maine Emergency Management Agency (MEMA)
- Department of Administrative and Financial Services - Office of Information Technology (OIT)

1.2 Supporting Agencies

- Maine Department of Public Safety (DPS)
  - Maine Information and Analysis Center (MIAC)
  - Maine State Police Computer Crimes Unit (MSPCCU)
  - Criminal Investigations Division (CID)
- Maine Department of Defense, Veterans, and Emergency Management (DVEM)
  - Maine National Guard (MENG)
- Department of Administrative and Financial Services
  - Office of Risk Management
- Multi-State – Information Sharing and Analysis Center (MS-ISAC)
- Maine Cyber Security Cluster (MCSC)

1.3 Table of Contents

Section 2: Purpose, Scope, Situation, and Assumptions

2.1 Purpose

The state of Maine's dependency on technology makes us susceptible to a large-scale cyber incident which could overwhelm government and private sector resources by disrupting the Internet and/or negatively impacting critical infrastructure information systems. Cyber disruptions of this magnitude may threaten lives, property, the economy, and national security. Rapid threat identification, information exchange, investigation, and coordinated response and remediation are critical to mitigate the damage caused by this type of malicious cyberspace activity.

The purpose of this annex is to define the concept of operations and the duties and responsibilities of the government in response to an incident involving systemic, cyber based attacks against computer and electronic systems that impact mission critical functions and or threaten public health or safety, undermine public confidence, have a debilitating effect upon the state of Maine or national economy, or diminish the security posture of the state of Maine or the Nation.

2.2 Scope

The scope of this annex describes the framework for state cyber incident response coordination among state departments and agencies. It may be utilized in any incident of State significance with cyber-related issues, including significant cyber threats and disruptions; crippling cyber-attacks against the Internet; Critical Infrastructure and Key Resource (CIKR) information systems; technological emergencies at any level within the state, local, or municipal government; or presidentially-declared disasters.

During certain response operations, this annex may be used in conjunction with affected agency incident response plans and the state Emergency Operations Plan, its annexes, and/or other planning documents as required. Cyber-related incidents of state significance may result in activation of the ESF-2, Communications; ESF-13, Public Safety and Security; ESF-15 External Affairs and the Cyber Incident Annex.

- **ESF-2** supports the restoration of the communication and information technology infrastructure, facilitates the recovery of systems and applications from cyber-attacks, and coordinates communications support to response efforts during incidents requiring a coordinated response.
- **ESF-12** provides coordination for emergency response measures in responding to and recovering from fuel shortages, power outages, and capacity shortages caused by an emergency incident, major disaster, acts of war, terrorism (physical or cyber), or civil disturbance in the state of Maine.
- **ESF-13** provides coordination for all state law enforcement resources to support local law enforcement before, during and following disasters.
- **ESF-15** provides the timely dissemination of emergency preparedness and response information to the general public, responders and elected or appointed officials.

2.3 Situation

- Maine's critical infrastructure and key resources consist of the physical and cyber assets of public and private institutions in several sectors: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear, transportation and water and waste water. Cyberspace allows all of these sectors to operate.

- Made-up of thousands of interconnected computers, servers, routers and switches, cyberspace is the backbone and infrastructure to our technology dependent society. Ensuring a healthy cyberspace is essential to our State's physical and economic prosperity. As our dependency on technology increases, cyber threats are becoming more prevalent and sophisticated. In today's society the source of a cyber-attack can be just a varied as the method.
- Cyber criminals, hacktivist and state-sponsored cyber actors all pose a significant threat to our critical infrastructure. A significant cyber incident could take many forms: an organized cyber-attack, an uncontrolled exploit such as a virus or worm, or a natural disaster with extensive damage to critical infrastructure or key assets. A successful cyber-attack is likely to affect mission critical functions and services across public and private sector domains. Cyber incidents may occur with little or no warning and may involve a variety of tactics which could affect critical state infrastructure and key resource sites. A cyber incident could rapidly overwhelm the ability of local, state, and federal agencies to respond to natural disasters as well as acts of terrorism.
- Maine shares several key infrastructure connections within the United States and Canada. No single agency at the local, county, state, or federal level possesses the authority and expertise to act unilaterally on the issues that could arise while responding to a cyber-attack or other cyber incident in the state of Maine.

2.4 Assumptions

- A cyber incident may occur at any time of day with little or no warning, may involve single or multiple geographic areas.
- MEMA will facilitate a coordinated response with federal counterparts.
- No single private or government agency at the local, tribal, state or federal level possesses the authority or expertise to act unilaterally. These agencies will work together on cyber related issues and response to lessen the effects of a cyber-related incident and/or terrorist act.
- The coordination with the federal government is dynamic and shaped by the nature of the event.
- Alternate and redundant telecommunications and information technology services will survive the effects of a cyber-attack (e.g., HAM Radios).
- Any Executive Branch state agency will notify OIT in the event of a cybersecurity incident affecting their IT systems.
- Most cyber events will not result in State Emergency Operations Center (SEOC) activation.
- When an incident occurs, county, local and tribal governments or private agencies will use their own response resources first, supplemented as needed by resources available through mutual aid or private sector contracts. Local governments will request state assistance when its ability to respond to the incident exceeds or is expected to exceed their own capacity.

Section 3: Concept of Operations

3.1 General

A cyber-related incident of state significance may take many forms: an organized cyber-attack, an uncontrolled exploit such as a virus or worm, a natural disaster with significant cyber consequences, or other incidents capable of causing extensive damage to critical infrastructure or key assets.

Large-scale cyber incidents may overwhelm government and private-sector resources by disrupting the Internet and/or taxing critical infrastructure information systems. Complications from disruptions of this magnitude may threaten lives, property, the economy, and national security. Rapid identification, information exchange, investigation, and coordinated response and remediation often can mitigate the damage caused by this type of malicious cyberspace activity.

Common cyber-threats include:

- Threats to individual systems such as phishing and spear phishing,
- Threats against information networks (e.g., hacking, network disruption, and exfiltration of sensitive information), and
- Threats to critical infrastructure (e.g., Supervisory Control and Data Acquisition [SCADA] systems, and Industrial Control Systems [ICS]).

3.2 Activities

Procedures in this annex are implemented when it is determined that a cyber-related incident of state significance is imminent or underway. The Cyber Security Incident Response Team (CSIRT) is convened and immediately notifies the National Cybersecurity and Communications Integration Center (NCCIC). Notification is made through established communications channels that exist between the MIAC and respective agencies.

a. Prevention and Protection

Steady-state activities: The wide variety of cyber-threats and the risks associated with them dictate unique mitigation strategies conducted on a day-to-day basis.

The following scalable and flexible strategies accommodate different threats across the whole community of cyber-users. Strategies to mitigate and protect against cyber-threats include:

- Ongoing public information campaigns by MEMA and OIT relating to cyber-safety for the public.
- Ongoing end-user training by computer and network owners on their IT policies, procedures, and established best practices to avoid network and proprietary data compromise.
- Ongoing network and internet monitoring and intelligence gathering by:
  - OIT staff routine monitoring of state networks.
  - MIAC monitoring of intelligence sources.
- Protective actions by individual computer users and network owners:
  - Use good computer hygiene to avoid exposing computers, data, and network resources to unauthorized persons and organizations.
  - Keep computer and network hardware and operating systems up to date.

  - Keep software licenses current as well as software patches and updates installed.
  - Regular information sharing with appropriate authorities.
- Intelligence gathering and analysis. State agencies share information on cyber-related threats with the MS-ISAC.

b. Response

i. Notification

Because of the pervasive nature of a cyber threat, initial identification of the threat may be through a variety of channels. Therefore, the state maintains three primary watch and warning centers that will monitor and share information in the event of a cyber-threat or attack:

- **MEMA Duty Officer (DO):** MEMA maintains a 24-hour duty officer who receives reports from individuals, state agencies, local units of government and the private sector. When notified of a cyber-threat or attack, the MEMA DO notifies the MEMA Director or Cyber Security Coordinator.
- **MIAC:** As the state of Maine's fusion center, the MIAC gathers information from numerous sources, and produces intelligence products for federal, state, and local government agencies, the private sector, and the public.
- **OIT Enterprise Security Team:** The Enterprise security team monitors the state cyber-domain for threats or disruptions using a variety of automated systems. OIT Enterprise security officer notifies the state chief information security officer of any detected or suspected threat or attack against state information technology assets.

ii. Cyber Security Incident Response Team Activation

Cyber-related mitigation and preparedness activities are ongoing functions that routinely occur as part of the steady-state operations.

Conditions which may trigger the incident response functions of this annex include:

- Major incident or disaster **(Table 1: Incident categories)**
- A threat or incident involving state-level cyber critical infrastructure, or
- An incident involving activation of state level continuity of operations (COOP), continuity of government (COG) plans, or
- When requested by:
  - A CSIRT member, or
  - MEMA Director, or
  - The Adjutant General (TAG), or
  - The Governor.
- Reference **Appendix A: CSIRT Incident Flow Chart**.

iii. State of Maine Cyber Security Incident Response Team (CSIRT)

CSIRT coordinates the response to any significant cyber event affecting the state of Maine technologies. This team will possess the required resources, authorities, and execution responsibilities that do not reside in one department, agency, organization, or company within the state of Maine.

Participants of the CSIRT will use their own authorities to assist response activities and are responsible for understanding and communicating the full range of capabilities that their organization brings to bear. The CSIRT will activate when notified by MEMA Director, or on request of another permanent member. The CSIRT includes the following permanent members and can be expanded as necessary based on the location and circumstances of the significant cyber incident:

- Director of Maine Emergency Management Agency (MEMA) or designated representative
- Associate CIO - Infrastructure, Office of Information Technology (OIT), state of Maine
- Director, Maine Information and Analysis Center (MIAC)
- Maine National Guard Director of Communications – J6
- Office of Risk Management

During a significant cyber incident, the CSIRT will provide guidance to the State Emergency Operations Center (SEOC) leadership. Examples of SEOC activities include:

- Establishing the incident response plan
- Ensuring overall coordination of significant cyber incident management and resource allocation activities
- Facilitating interagency conflict resolution or elevating matters, as necessary
- Coordinating response between multiple cyber incidents when applicable
- Ensuring the Governor’s Office and SEOC receive timely updates on the status of response activities
- Coordinating external affairs activities

Appendix A: CSIRT Activation Flowchart

iv. Incident Categories and Actions

As with mitigation strategies, response to a cyber-incident must be scalable and flexible. Since each cyber-threat or incident is unique, CSIRT, OIT or MEMA may adjust the scale of the response, as follows:

Table 1: Incident Categories

Category	Events	Response
Minor Incident	• Isolated incidents that reduce functionality of organization; • Service outages; • Persistent low level cyber activity (phishing, network probing, etc.)	• Steady State operations; • MEMA DO monitoring with CSIRT information sharing; • MIAC may request additional resources; • Assess need to upgrade to Major Incident Response.
Major Incident	• Incidents that degrade/destroy functionality of an organization; • Prolonged service outage; • Confirmed Data Breach or Data theft; • Any cyber event that exceeds the affected agency capacity to manage incident response.	• MEMA DO will monitor incident; • CSIRT activation to coordinate response; • SEOC may be activated; • MIAC and OIT manage outside resource requests as needed; • Assess need to upgrade to Disaster Response.
Disaster	• Incidents that destroy all functionality of organization; • Coordinated cyber-attack with direct impact on citizens; • Terrorist attack or accidental destruction of critical infrastructure.	• State declaration of emergency, • CSIRT manages cyber response, • SEOC activated to manage physical world effects; • Implement mutual aid agreements & COOP; • request outside assistance as required through MIAC and OIT.
Consistent with OIT Major Incident Procedure – dated Feb 26, 2014; Rev. Aug. 6, 2015		

For a national-level Significant Cyber Incident, US DHS, through the NCCIC, coordinates national response efforts and works directly with state, local, and tribal governments and the private sector.

Section 4: Responsibilities

4.1 Lead Agencies

The responsibility for lead agency will depend on the particular branch of state government that is impacted. Co-lead agencies are expected to coordinate and manage cyber incident response and share information to members of the Cyber Security Incident Response Team (CSIRT) and provide information sharing to affected parties.

a. Executive Branch

The state of Maine Office of Information Technology (OIT) within the Executive Branch maintains the most resources and knowledge and is best suited to lead the coordination within their respective branch. Should the resources of the OIT be exceeded and/or if the cyber incidents are widespread enough that a coordinated Federal response is required, OIT will notify MEMA to request the necessary resources.

Office of Information and Technology

As the lead agency for the state of Maine Executive Branch, OIT has a number of responsibilities in dealing with cyber incidents. They are primarily responsible for identifying state cyber incidents on state government systems. They also notify the Multi-State Information Sharing & Analysis Center (MS-ISAC), CSIRT members, affected commissioner, and affected agency as soon as possible. In order to prepare for cyber incidents, they also must review, maintain, and operate within their incident response plan (See Appendix B OIT Enterprise Security Procedures Flowchart).

As the primary agency for Executive Branch cyber threats and/or incident response, OIT is responsible for state-level coordination of assets and services and will accomplish the following:

- Identifying and coordinating support-function staffing requirements appropriate to the emergency situation to include coordination of the CSIRT.
- Coordinating response to requests for assistance from the affected agencies.
- Assisting in documentation preparation for departmental funding needs and develop priorities for state resource allocation.
- Assisting in coordinating and monitoring state funded remediation efforts.
- Obtaining and compiling documentation/information necessary for effective and efficient strategy management by MEMA SEOC staff
- In coordination with MEMA, develop, maintain, and distribute this and any appropriate SOPs.

b. All State Levels

The Maine Emergency Management Agency (MEMA) provides outreach to all branches and levels of government within the state and is the best resource for cyber incident response coordination.

Maine Emergency Management Agency

Serves as the primary agency for all non-executive branch state-wide cyber incidents their ongoing responsibilities include:

- Identify incident if reported by public/private industry or non/state level government

- Activate Cyber Security Incident Response Team (CSIRT)
- Coordinate CSIRT/SEOC staffing and functioning
- Manage resources through Emergency Support Functions, if SEOC is activated
- Facilitate information sharing
- Support actions/notifications to local, state and federal partners
- Declare emergency thresholds and expense reimbursement
- Request Maine National Guard (MENG) Cyber Response Team (CRT)

4.2 Supporting Agencies

All responsible agencies will be aware of their organization's capabilities for providing assistance and support. Supporting agencies will provide assistance in the form of personnel, equipment, and/or technical assistance as requested by the Primary Agency, CSIRT, and/or MEMA.

a. Department of Public Safety

DPS has several divisions that assist with criminal cyber investigations:

i. Maine Information and Analysis Center (MIAC)

MIAC supports crime investigations and special cases to the federal, state, county and local law enforcement. The division provides real-time intelligence support to law enforcement and public safety authorities, and consolidates information and data on suspicious activities and threats from all jurisdictions and disciplines as well as the public. During emergencies or periods of increased threat, the MIAC may ramp up to receive and process additional information. Responsibilities include:

- Identify incident if reported to MIAC or E911 by public/private industry
- Notify MEMA and MSPCCU
- Notify DHS, USSS, FBI, and public/private sector partners as needed
- Support the lead agency in response to a cyber-incident
- Gather and disseminate threat intelligence
- Coordinate criminal investigation – provide oversight for evidence collection

ii. Maine State Police Computer Crimes Unit

Based at the Maine Criminal Justice Academy in Vassalboro, ME and with satellite forensics labs in Lewiston and Bangor, the Computer Crimes Unit investigates computer crimes, provides computer forensics services, and provides training, technical support and legal support to law enforcement officers and prosecutors throughout the state. The Computer Forensics Unit and Cyber Crimes Unit will support and provide assistance, at the request of the primary agency, with the investigation and prosecution of computer security breaches involving suspected malicious or damaging computer intrusions that violate Aggravated Criminal Invasion of Computer Privacy, Statute: 17-A, Section 433.

iii. The Criminal Investigations Division

CID manages the Computer Information Technology & Electronic Crime (CITEC) program. The CITEC agent pursues investigations, data recovery and analysis on computer systems and/or the Internet which are used to facilitate a crime or to store evidence of a crime. Investigations include network intrusions, denial-of-service attacks, web site defacements, child pornography, gambling, and terrorist (e-mail) threats, tampering with a government record, and identity theft or fraud.

b. Maine National Guard (MENG)

The Maine National Guard maintains a high level of computer network capability in order to maintain their own IT infrastructure throughout the state of Maine. The capability of their equipment and personnel are available to support domestic operations, as may be directed by the Governor of Maine through the Commissioner, Department of Defense, Veteran's, and Emergency Management, as authorized by statute and in accordance with the SEOP. These capabilities could include network support and guidance to affected agencies, vulnerability assessment, cyber incident response and recovery actions, as well as equipment requests to maintain connectivity during a cyber-attack. All National Guard missions will be requested by MEMA or SEOC then validated and approved by the MENG Joint Operations Center. Additionally the Maine National Guard Director of Communications – J6, will provide expertise and guidance as a member of the CSIRT on MENG capability and resources during a cyber incident.

c. Maine Cyber Security Cluster (MCSC)

The Maine Cyber Security Cluster (MCSC) in partnership with the University of Maine System has industry partners and academic resources to assist in a federal, state, or local cyber related emergency. Future capability will include faculty, students, and a lab environment to function as an education and prevention resource through training opportunities and vulnerability testing.

4.3 Federal Resources

a. Multi-State Information Sharing and Analysis Center

The MS-ISAC is a key resource for state, local, tribal and territorial (SLTT) government for cyber threat prevention, protection, response and recovery. The MS-ISAC 24/7 cybersecurity operations center provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification, and mitigation and incident response.

MS-ISAC facilitates cross-sector communication and information sharing for all sectors of critical infrastructure. Additionally, the MS-ISAC can respond to a cyber incident to assist state and local governments as well as provide immediate advice and coordination via conference calls during a major event.

b. Department of Homeland Security

When cyber incidents occur, the Department of Homeland Security (DHS) can provide assistance to impacted entities, analyze the potential impact across critical infrastructure, investigate those responsible in conjunction with law enforcement partners, and coordinate the national response to significant cyber incidents. DHS works in close coordination with other agencies with complementary cyber missions, as well as private sector and other non-federal owners and operators of critical infrastructure, to ensure greater unity of effort and a whole-of-nation response to cyber incidents.

i. National Cybersecurity and Communications Integration Center

A 24/7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the federal government, intelligence community, and law enforcement.

- United States Computer Emergency Readiness Team (US-CERT) brings advanced network and digital media analysis expertise to bear on malicious activity targeting our nation's networks. US-CERT develops timely and actionable information for distribution to federal departments and agencies, state and local governments, private sector organizations, and international partners.
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT**)** works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Cybersecurity and infrastructure protection experts from ICS-CERT provide assistance to owners and operators of critical systems by responding to incidents and helping restore services, and by analyzing potentially broader cyber or physical impacts to critical infrastructure. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.
- National Cybersecurity Assessment and Technical Services (NCATS) offers cybersecurity scanning and testing services that can identify vulnerabilities within networks and provide risk analysis reports with actionable remediation recommendations. These services provide proactive mitigation to exploitable risks and include network (wired and wireless) mapping and system characterization; vulnerability scanning and validation; threat identification and evaluation; social engineering, application, database, and operating system configuration review; and incident response testing.
- National Coordinating Center for Communications (NCC) leads and coordinates the initiation, restoration, and reconstitution of national security and emergency preparedness telecommunications services and/or facilities under all conditions.

ii. Critical Infrastructure Cyber Community Voluntary Program (C^{3}VP)

The coordination point within the federal government for critical infrastructure owners and operators interested in improving their cyber risk management processes. The C^3 Voluntary Program aims to support industry in increasing its cyber resilience; increase awareness and use of the Framework for Improving Critical Infrastructure Cybersecurity; and encourage organizations to manage cybersecurity as part of an all hazards approach to enterprise risk management.

c. Department of Justice - Federal Bureau of Investigation

The FBI serves as the national focal point for coordinating cyber threat investigations. Through the National Cyber Investigative Joint Task Force (NCIJTF) the FBI enhances collaboration and integrates operations among the represented U.S. Intelligence Community and federal law enforcement partners against:

- Cyber terrorists exploiting vulnerabilities in critical infrastructure control systems
- Nation-state theft of intellectual property and trade secrets
- Financially-motivated criminals stealing money, identities, or committing cyber extortion
- Hactivists illegally targeting businesses and government services
- Insiders conducting theft and sabotage

The FBI developed a Cyber Task Force (CTF) in all 56 field offices to assist state and local agencies on combating cyber threats. These CTFs promote collaboration with local and national agencies and can provide the following resources:

- Cyber incident response investigations
- Addressing Cyber threat, vulnerabilities and collection methods
- Relation building and information sharing for public/private sector
- Subject Matter Expertise for research and instruction

Additionally, the FBI has developed a Cyber Action Team (CAT), comprised of 50 members around the country that possess advance knowledge in computer scripting languages, forensic investigations and malware analysis. This team can rapid deploy anywhere in the world within 48 hours providing investigations support. Their ability to analyze the tools, techniques, and procedures (TTPs) that hackers use aid in the attribution of cyber actors leading to the eventual arrest.

d. Cyber Crime

i. The U.S. Secret Service maintains Electronic Crimes Task Forces, which focus on identifying and locating international cyber criminals connected to cyber intrusions, bank fraud, data breaches, and other computer-related crimes. The Secret Service's Cyber Intelligence Section has directly contributed to the arrest of transnational cyber criminals responsible for the theft of hundreds of millions of credit card numbers and the loss of approximately $600 million to financial and retail institutions. The Secret Service also runs the National Computer Forensic Institute, which provides law enforcement officers, prosecutors, and judges with cyber training and information to combat cyber-crime.

ii. The U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Cyber Crimes Center (C3) delivers computer-based technical services to support domestic and international investigations into cross-border crime. C3 is made up of the Cyber Crimes Unit, the Child Exploitation Investigations Unit, and the Computer Forensics Unit. This state-of-the-art center offers cyber-crime support and training to federal, state, local, and international law enforcement agencies. C3 also operates a fully equipped computer forensics laboratory, which specializes in digital evidence recovery, and offers training in computer investigative and forensic skills.

iii. The Law Enforcement Cyber Incident Reporting resource provides information for SLTT law enforcement on when, what and how to report a cyber incident to a federal entity. The document also provides information on federally sponsored training opportunities and other useful resources available to SLTT law enforcement.

Section 5: Supplementary and Procedural Documents

- Maine National Guard Joint Operations Plan, Domestic Operations, Annex K Cyber Response
- Notice of Risk to Personal Data Act, Jan. 1, 2006, (www.maine.gov)
- State of Maine Department of Administrative and Financial Services, Office of Information Technology, Major Incident Procedures (http://www.maine.gov/oit/policies/)

Section 6: References

- An Order Establishing the Maine Intelligence Analysis Center, 24FY 06/07, December 8, 2006 Threats to the Homeland and Americans Overseas (Classified) (www.maine.gov)
- An Order Establishing the State of Maine Information Protection Working Group and For Other Purposes, 2014-0003, July 17, 2014. (www.maine.gov)
- Cybersecurity Information Sharing Act of 2015, S.754 (www.congress.gov)
- Executive Order 12333: United States Intelligence Activities, as amended (www.cia.gov)
- Executive Order 12472: The Assignment of National Security Emergency Preparedness Responsibilities for Telecommunications (www.whitehouse.gov)
- Executive Order 13636: Improving Critical Infrastructure Cybersecurity (www.whitehouse.gov)
- Federal Information Security Management Act (FISMA) (csrc.nist.gov)
- Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, Feb. 12, 2014. (http://www.nist.gov/cyberframework/)
- Homeland Security Presidential Directive-5 (HSPD-5) (www.dhs.gov)
- Homeland Security Presidential Directive-7 (HSPD-7) (www.dhs.gov)
- Maine Revised Statute Title 37B, Chapter 13: Maine Emergency Management Agency (legislature.maine.gov)
- National Security Act of 1947, as amended (legcounsel.house.gov)
- National Security Directive 42: National Policy for the Security of National Security Telecommunications and Information Systems (fas.org)
- National Strategy to Secure Cyberspace (www.us-cert.gov)
- Presidential Policy Directive 21 (PPD-21) (www.whitehouse.gov)
- Section 706, Communications Act of 1934, as amended (47 U.S.C. 606) (www.law.cornell.edu)
- The Defense Production Act of 1950, as amended (www.fema.gov)
- The Enhancement of Non-Federal Cyber Security, The Homeland Security Act (legcounsel.house.gov)
- The Robert T. Stafford Disaster Relief and Emergency Assistance, Public Law 93-288 as amended. (www.fema.gov)

Section 7: Appendices

Appendix A: CSIRT Activation Flowchart

This document is For Official Use Only and can be accessed upon credible request through MEMA's webpage (http://www.maine.gov/mema/).

Appendix B: OIT Enterprise Security Procedures Flowchart

This document is For Official Use Only and can be accessed upon credible request through MEMA’s webpage (http://www.maine.gov/mema/).